



Vendor: Splunk

Exam Code: SPLK-5003

Exam Name: Splunk Certified Cybersecurity Defense

Architect

Version: DEMO

QUESTION 1

A cybersecurity team is looking to leverage DevSecOps best practices. They want to test new security policies with a small subset of users while monitoring for unusual access patterns or failures. Which of the following techniques will support this? (Choose all that apply.)

- A. Infrastructure-as-Code
- B. Blue-Green Deployments
- C. Canary Releases
- D. Automated Rollbacks

Answer: CD

Explanation:

Canary releases allow new security policies to be introduced gradually to a small subset of users while monitoring for access issues, failures, or unexpected behavior. Automated rollbacks support this approach by quickly reverting the change if the monitored results show problems, reducing operational risk during policy deployment.

QUESTION 2

Carter is an architect at an organization drafting design and support documents for a net new SOAR deployment. What does Carter have to take into consideration? (Choose all that apply.)

- A. SOAR deployment can connect to the required destinations.
- B. Write a request for proposal.
- C. The organization has an agreed upon RACI.
- D. RBAC controls have been properly defined.

Answer: ACD

Explanation:

A SOAR deployment must be designed with reliable connectivity to the systems it will orchestrate, clear ownership of operational responsibilities, and properly defined role-based access controls. These considerations ensure playbooks can execute actions safely, teams understand accountability, and users have only the permissions needed for their roles.

QUESTION 3

Brian is a security architect at an organization and wants to test the efficacy of the security controls currently being used. Which of the following is the best way this can be achieved?

- A. Establish a Red vs Blue program
- B. Establish a Red vs Purple program
- C. Establish a Blue vs Blue program
- D. Establish a Blue vs Purple program

Answer: B

Explanation:

A Red vs Purple program is best for testing security control efficacy because adversary-style testing is paired with collaborative analysis and tuning. This helps validate whether existing controls detect, prevent, and support response to realistic attack behaviors while improving defensive coverage.

QUESTION 4

Which of the following best explains how quantifying the financial impact of a cybersecurity

incident can help justify and secure additional budget for the cybersecurity team? (Choose all that apply.)

- A. It demonstrates the potential cost savings by preventing incidents, making a strong business case for increased funding.
- B. It indicates that only technical improvements matter, not financial considerations.
- C. It shows that cybersecurity incidents are unavoidable, so additional budget is necessary.
- D. It highlights that cybersecurity spending should be reduced to save costs.

Answer: A

Explanation:

Quantifying financial impact translates cybersecurity risk into business terms, showing how investment can reduce expected losses from incidents. This makes it easier to justify additional budget by demonstrating potential cost avoidance, risk reduction, and measurable business value.

QUESTION 5

How can an organization's identity and access management (IAM) architecture enable security orchestration?

- A. IAM system logs provide valuable alerts for security orchestration.
- B. Allows normal users to bypass IAM controls for faster response to authentication and authorizations.
- C. Provides granular permissions to automate disabling accounts, resetting passwords, or changing privileges.
- D. Performs changes to IAM system settings to alter authentication methods.

Answer: C

Explanation:

IAM architecture enables security orchestration by allowing automated response actions with controlled, granular permissions. This lets SOAR workflows safely disable accounts, reset passwords, revoke sessions, or modify privileges during an investigation or containment process.

QUESTION 6

A SOC engineer, is evaluating how to use artificial intelligence in order to improve how their organization responds to security threats. Which of the following benefits can the engineer realize from augmenting incident response with artificial intelligence?

- A. AI will require security analysts to spend more time writing detection rules.
- B. AI will automatically respond to and remediate all security events without supervision.
- C. AI can write incident reports that analysts do not need to review before publishing.
- D. AI can reduce the amount of time analysts spend collecting and correlating data from security tools.

Answer: D

Explanation:

Artificial intelligence can improve incident response by helping analysts gather, normalize, summarize, and correlate information across multiple security tools faster. This reduces manual investigation effort and allows analysts to focus more time on validation, decision-making, and response actions.

QUESTION 7

In a DevSecOps workflow, what is the primary purpose of an automated security gate that detects critical vulnerabilities during a build or deployment?

- A. To provide developers with optional warnings about potential security risks without affecting the build or deployment process.
- B. To replace manual security audits and eliminate the need for developer security training.
- C. To accelerate the software release cycle by bypassing security checks for minor issues.
- D. To ensure that only code meeting defined security standards is deployed to production, automatically failing the build or deployment if critical issues are found.

Answer: D

Explanation:

An automated security gate enforces defined security standards during the build or deployment pipeline. When critical vulnerabilities are detected, it automatically blocks the release so insecure code is not promoted to production.

QUESTION 8

An organization seeks to improve its cybersecurity posture and risk management strategy by implementing and adhering to NIST CSF Functions (Identify, Protect, Detect, Respond, Recover, Govern) as a shared set of practices and standard vocabulary. In what order should these CSF functions be addressed?

- A. In CSF provided order (first to last)
- B. Concurrently
- C. In a cyclical manner
- D. As needed

Answer: B

Explanation:

NIST CSF Functions are intended to be addressed concurrently as part of an integrated cybersecurity risk management approach. The functions work together to provide a shared structure for managing cybersecurity outcomes rather than a strict step-by-step sequence.

QUESTION 9

A national retail chain is planning to implement a SIEM to improve its PCI compliance in response to an audit finding. What is a benefit that the SIEM should provide to the organization?

- A. Cardholder data is encrypted both in transit and at rest using the latest TLS and AES standards to prevent eavesdropping.
- B. Access to cardholder networks and system resources is monitored continuously, and alerts are produced in the case of access anomalies.
- C. Card transactions are recorded in a central location for financial reporting.
- D. Security controls are routinely tested to ensure they are implemented correctly and continue to function properly.

Answer: B

Explanation:

A SIEM supports PCI compliance by continuously monitoring access to cardholder data environments, collecting security-relevant logs, correlating activity, and generating alerts for anomalous or unauthorized access. This helps the organization detect and investigate potential security events affecting cardholder networks and systems.

QUESTION 10

Yokoco has contracted with Helpime to perform a penetration test. The scope of the test is all web facing internet applications. Helpime has completed the test and provided its report to Yokoco. What should be done with the unremediated findings of this report?

- A. They should be shared with regulatory authorities to add to their risk register.
- B. They should be entered and tracked in the risk register.
- C. They should be reviewed and saved for future reference.
- D. They should immediately be shared with all teams that are affected.

Answer: B

Explanation:

Unremediated penetration test findings represent known security risks that must be formally documented, assigned ownership, prioritized, and tracked through remediation or risk acceptance. Entering them in the risk register ensures they remain visible and managed within the organization's risk management process.

QUESTION 11

The internet facing WAF for a new customer facing application has been identified as a potential telemetry collection point. Which of the following best describes this data prior to any tuning or curation efforts?

- A. High Value/Low Noise
- B. High Value/High Noise
- C. Low Value/High Noise
- D. Low Value/Low Noise

Answer: B

Explanation:

Internet-facing WAF telemetry is high value because it provides visibility into attacks, suspicious requests, exploit attempts, and traffic patterns targeting a customer-facing application. Before tuning or curation, it is also typically high noise because public-facing applications receive large volumes of benign traffic, automated scanning, false positives, and repetitive web requests.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14